Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

24738 7590 03/22/2006

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
INTELLECTUAL PROPERTY & STANDARDS
1109 MCKAY DRIVE, M/S-41SJ
SAN JOSE, CA 95131

EXAMINER	
DINH, MINH	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/749,142	**Applicant(s)** WILLE ET AL.	
	Examiner Minh Dinh	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4 and 6-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *2,4,7-24,27 and 28* is/are rejected.

7)☒ Claim(s) *3,6,25 and 26* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 01/03/2006. Claim 28 has been amended.

Response to Arguments

2. Applicant's arguments, see paragraph e, page 9, with respect to claims 3, 6 and 25-26 under 35 USC 103(a) have been fully considered and are persuasive. The rejections of claims 3, 6 and 25-26 under 35 USC 103(a) have been withdrawn.

3. Applicant's arguments with respect to claims 2, 4 and 8-14 have been considered but are not persuasive have been fully considered but they are not persuasive.

Applicant argues that nowhere does the Action set forth suggestion or motivation in Patarin, Jahnich or Tan to properly support the Action's conclusion that it would be obvious to modify Patarin based on Jahnich or Tan (paragraph a, page 8). Suggestion or motivation to modify Patarin based on Jahnich or Tan was provided in paragraphs 12-13 in the previous Office Action.

Applicant argues that the Action uses the claimed inventions as a "road map" to gather various parts from Patarin, Jahnich and Tan, but does not deal with issues as to whether Paritan can be modified at all or whether Jahnich dummy operations can be run simultaneously and in parallel with a useful operation (paragraphs b-d, page 9). Patarin discloses that his method and system deal with any sequential or successive cryptographic process (col. 3, lines 32-38). Jahnich teaches that execution of the dummy operations in a sequential cryptographic process does not influence the result of a cryptographic operation, but causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker (col. 6, lines 32-37). Thus the teaching of the prior arts provides a sufficient basis for a reasonable expectation of success.

Applicant argues that nowhere does the Action succeed in gathering parts that meet Applicant's element/arrangement in splitting of useful operations in a random manner. Attention is directed to the first full paragraph in page 9 of the previous Office Action where the limitation recited in claim 8 "the split-up of the cryptographic operation into sub-operations is random-controlled" is addressed. Claim 14 is rejected on the same basis as claim 8.

4. Applicant's arguments with respect to claims 15-18, 20-24 and 28 have been fully considered but they are not persuasive. Applicant argues that the Action omits to identify where Patarin discloses, or even contemplates, operations performed "simultaneously and in parallel" so that "consumption characteristics of the data-processing device is a superimposition of consumption characteristics" associated with each operation (page 11, 2nd paragraph). Although Patarin does not explicitly disclose the feature, it is deemed to be inherent as Patarin discloses a smart card comprising multiple processors which perform cryptographic operations in parallel; and therefore,

the current consumption characteristics of the smart card is a superimposition of consumption characteristics of each processor in the smart card.

Applicant argues that nowhere does the Action set forth any sufficient suggestion or motivation from Patarin or Ohki to support the Action's conclusion that it would, be obvious to modify Patarin's complex process to use "the dummy programs of Jahnich" (page 11, 3rd paragraph). It is assumed that the reference to "the dummy programs of Jahnich" is a mistake because Patarin is combined with Ohki in the rejection of claim 15. Attention is directed to the page 10 of the previous Office Action where sufficient motivation is provided to support the Action's conclusion that it would be obvious to modify Patarin's to use a complimentary operation taught by Ohki.

Applicant argues that there is no basis for a "reasonable expectation of success" in the combination of Pantarin and Ohki (page 11, last paragraph). Patarin discloses that his method and system deal with any sequential or successive cryptographic process (col. 3, lines 32-38). Ohki teaches that execution of the complimentary operations in a sequential cryptographic process does not influence the result of a cryptographic operation, but reduces the dependency of current consumption upon data process (col. 2, line 36 – col. 3, line 6). Thus the teaching of the prior arts provides a sufficient basis for a reasonable expectation of success.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Regarding claim 28, the phrase "other timing characteristics" renders the claim indefinite because the mete and bound of the phrase "other timing characteristics" are not clear. The phrase will not be considered in the prior art rejection below.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 4, 7, 9 and 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin et al. (6,658,569) in view of Jahnich et al. (6,725,374).

Regarding claims 2 and 10, Patarin discloses a device comprising a central processing unit and one or more co-processors for performing cryptographic operations simultaneously and in parallel (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40). Patarin does not teach the use of dummy operations when performing a cryptographic operation. Jahnich discloses using dummy operations, whose execution does not influence an encryption result and that the consumption characteristics generated by the dummy operation is part of the consumption characteristics of the smart card when executing the cryptographic operation and the dummy operation so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (col. 6, lines 29-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Patarin to use dummy operations when performing a cryptographic operation, as taught by Jahnich, so that reconstruction of the consumption characteristics associated with performing the cryptographic operation would be impeded. Accordingly, the dummy operation is performed in parallel and simultaneously with the cryptography operations.

Regarding claims 4, 7, 11-13, Patarin further discloses that the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously, while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (figures 3a-b).

9. Claims 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 7 and 13 above, and further in view of Tan (6,490,353). Patarin and Jahnich do not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42);

the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

10. Claims 15-18, 20-24 and 28 rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Ohki et al (6,839,847).

Regarding claims 15-16, 18, 20, 22, 24 and 28, Patarin discloses a method of performing a cryptographic operation in a device, the device including at least two processors; the method comprising: performing a cryptographic operation in a first processor; performing a second operation in a second processor, the second operation being performed simultaneously and in parallel with performing the cryptographic operation so that consumption characteristics of the device is a superimposition of consumption characteristics associated with performing the cryptographic operation and consumption characteristics associated with performing the second operation (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40). Patarin does not disclose that the second operation associated with consumption characteristics complementary to consumption characteristics associated with the cryptographic operation. Ohki discloses a device performing two operations: a cryptographic operation using normal input data and another operation using inverted input data, such that the power consumption of the device remains constant (col. 2, line 36 – col. 3, line 6), the Ohki operations meets the limitation that power consumption characteristics associated with one operation is complementary to that associated with the other. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Patarin method such that the power consumption characteristics associated with one operation is complementary to that associated with the other operation, as taught by Ohki, in order to reduce the correlation/dependency between data processing and the current consumption of an IC card.

Regarding claim 17, the claim limitation is interpreted as that the consumption characteristics associated with the cryptographic operation is concealed by the consumption characteristics of the device (see Specification, p. 5, line 32 – p. 6, line 5). Claim 17 is rejected on the same basis as claim 15 above.

Regarding claims 21 and 23, Patarin further discloses that the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously, while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

11. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin and Ohki as applied to claims 15 and 18 above, and further in view of Qiu et al. (6,804,782). Patarin and Ohki do not disclose using a key that creates the complementary current variation. Qiu discloses using dummy operations to disguise power consumption and processor cycle time to prevent power attack and timing attack

on cryptographic operations. Qiu further discloses using a key which triggers the dummy operations so as to result in a complementary current variation (Abstract; col. 1, lines 46-54; col. 2, lines 39-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Patarin and Ohki to use using a key that creates the complementary current variation, as taught by Qiu. The motivation for doing so would have been to prevent both power and timing attacks simultaneously. Since frequency is calculated using the processor cycle time, inherently, reconstruction of consumption characteristics associated with the cryptographic operation using frequency is impeded.

Allowable Subject Matter

12. Claims 3, 6 and 25-26 are objected to as being dependent upon a rejected base claim, but would be allowable over the prior arts of record if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,327,661 to Kocher et al.

U.S. Patent No. 6,419,159 to Odinak

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
3/17/06

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100